(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年4 月28 日 (28.04.2005)

PCT

(10) 国際公開番号
WO 2005/039102 A1

(51) 国際特許分類[7]: H04L 9/20, 9/32

(21) 国際出願番号: PCT/JP2004/015493

(22) 国際出願日: 2004 年10 月20 日 (20.10.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2003-359849
2003 年10 月20 日 (20.10.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社イソップ (AESOP CORPORATION) [JP/JP]; 〒4600017 愛知県名古屋市中区松原二丁目４番１４号 Aichi (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 岩田清 (IWATA, Kiyoshi) [JP/JP]; 〒4600017 愛知県名古屋市中区松原二丁目４番１４号 株式会社イソップ内 Aichi (JP).

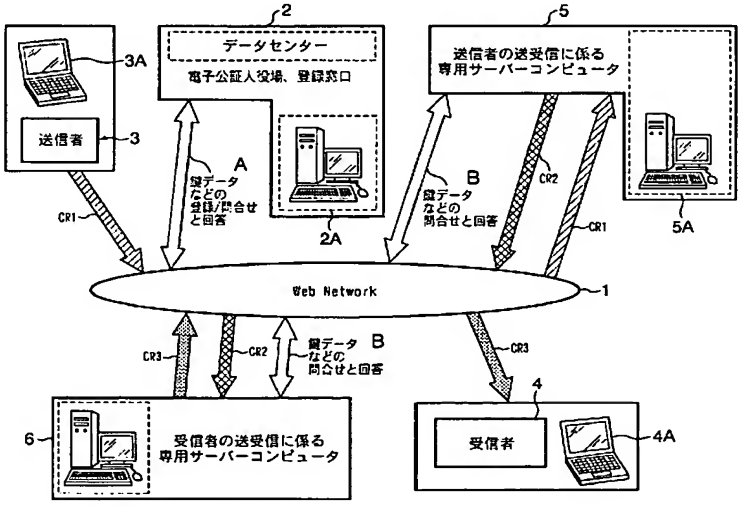
(74) 代理人: 樋口盛之助，外(HIGUCHI, Morinosuke et al.); 〒1050001 東京都港区虎ノ門５丁目１３番１号 虎ノ門４０ＭＴビル Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: INFORMATION ENCRYPTION TRANSMISSION/RECEPTION METHOD

(54) 発明の名称: 情報の暗号化送受信方法



3... SENDER
2... DATA CENTER (ELECTRONIC NOTARY PUBLIC OFFICE, REGISTER WINDOW)
5... DEDICATED SERVER COMPUTER RELATED TO TRANSMISSION/RECEPTION BY SENDER
A... REGISTER OF KEY DATA AND THE LIKE/INQUIRY AND REPLY THEREOF
B... ENQUIRY AND REPLY OF KEY DATA AND THE LIKE
6... DEDICATED SERVER COMPUTER RELATED TO TRANSMISSION/RECEPTION BY RECEIVER
4... RECEIVER

(57) Abstract: A sender uses his or her own key to encrypt data and send it to a data center (2). After using the sender's key to decrypt the encrypted data, the data center (2) uses the sender's key to re-encrypt it and sends it to a receiver (4). The receiver uses his or her own key to decrypt the re-encrypted data to obtain the original data. In this way, an encryption communication can be performed. It should be noted that an encryption algorithm used in the present invention is a bit unit XOR operation of plaintext and key.

[続葉有]

WO 2005/039102 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

規則4.17に規定する申立て:
— *US*のみのための発明者である旨の申立て (規則 *4.17(iv)*)

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

送信者はデータを自己の鍵で暗号化し、データセンター２に送る。データセンター２は、暗号化データを送信者の鍵を使って復号した後、受信者の鍵で再暗号化し、受信者４に送信する。受信者は自己の鍵でその再暗号化データを復号し、元のデータを得ることで、暗号化通信を行うことができる。尚、本発明で用いられる暗号アルゴリズムは平文と鍵とのビット単位ＸＯＲ演算である。